ΥΠΟΛΟΓΙΣΤΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΙΑ

Εισαγωγή

Άρης Παγουρτζής – Στάθης Ζάχος
Σχολή ΗΜΜΥ ΕΜΠ

Διοικητικά του μαθήματος

- Διδάσκοντες
  - Στάθης Ζάχος
  - Άρης Παγουρτζής
- Βοηθοί διδασκαλίας
  - Δημήτρης Σακαβάλας
  - Παναγιώτης Γροντάς
  - Γιώργος Παναγιωτάκος
  - Διονύσης Ζήνδρος
- Ημέρες-ώρες
  - Δευτέρα 10:45-12:30
  - Παρασκευή 12:45-14:30

Διοικητικά του μαθήματος

- Ιστοσελίδα:
  - http://www.corelab.ntua.gr/courses/crypto
- Βαθμολογικό σχήμα:
  - Ασκήσεις: 2 μονάδες
  - Εργασία μεγάλη (project): 2 μονάδες
  - Εργασία μικρή: 1 μονάδα
  - Τελικό διαγώνισμα: 6 μονάδες (απαραίτητες 2)

Τι είναι η Κρυπτογραφία

- Πιο σωστά: Κρυπτολογία
- Η τέχνη της «μεταμφίεσης» της πληροφορίας (*κρυπτογράφηση*)
- ...αλλά και της επαναφοράς της στην αρχική μορφή (*αποκρυπτογράφηση*)
- ...ακόμη και χωρίς το νόμιμο κλειδί (*κρυπτανάλυση*)
- ... και όχι μόνο: ψηφιακές υπογραφές, ταυτοποίηση, ψηφοφορίες, ασφαλείς υπολογισμοί, ψηφιακό χρήμα, ...

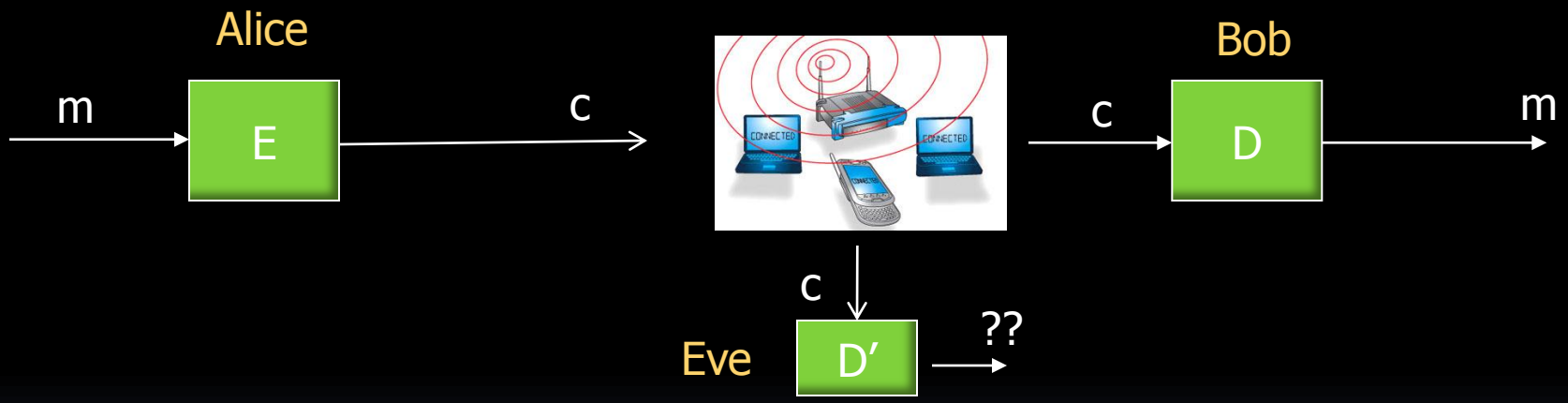
Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση

Αποκρυπτογράφηση

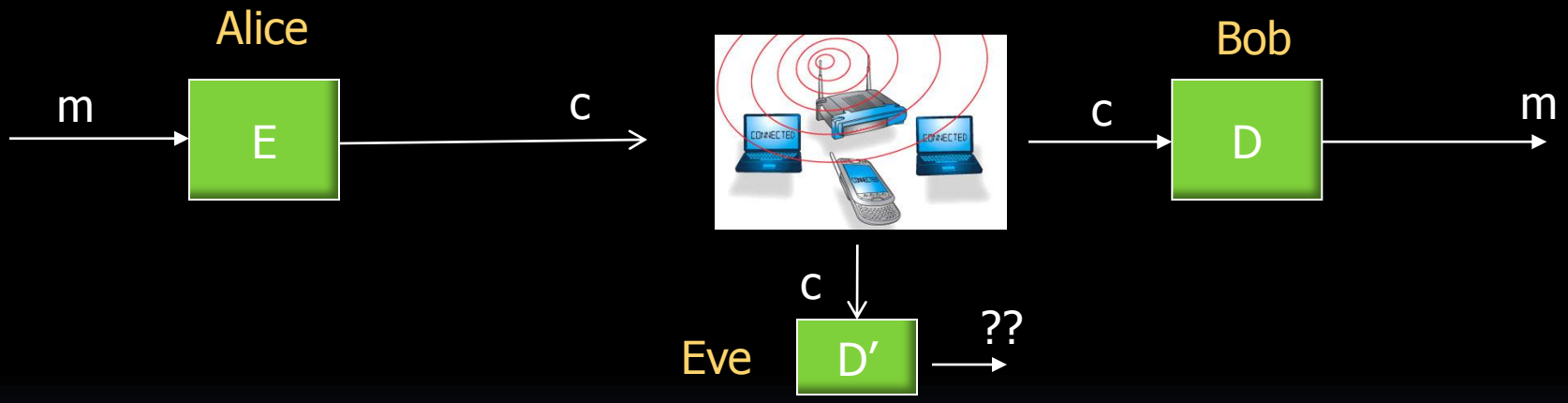
Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση Αποκρυπτογράφηση



Μια πρώτη ματιά: ιδιωτικότητα

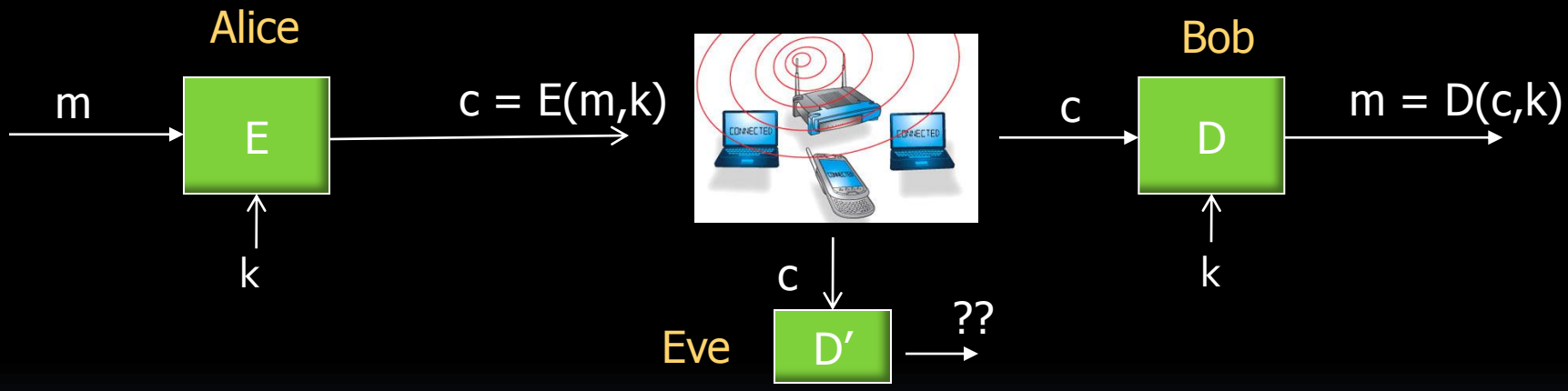
Κρυπτογράφηση Αποκρυπτογράφηση



- … με χρήση *κοινού* ιδιωτικού κλειδιού (συμμετρική κρυπτογραφία)

Μια πρώτη ματιά: ιδιωτικότητα

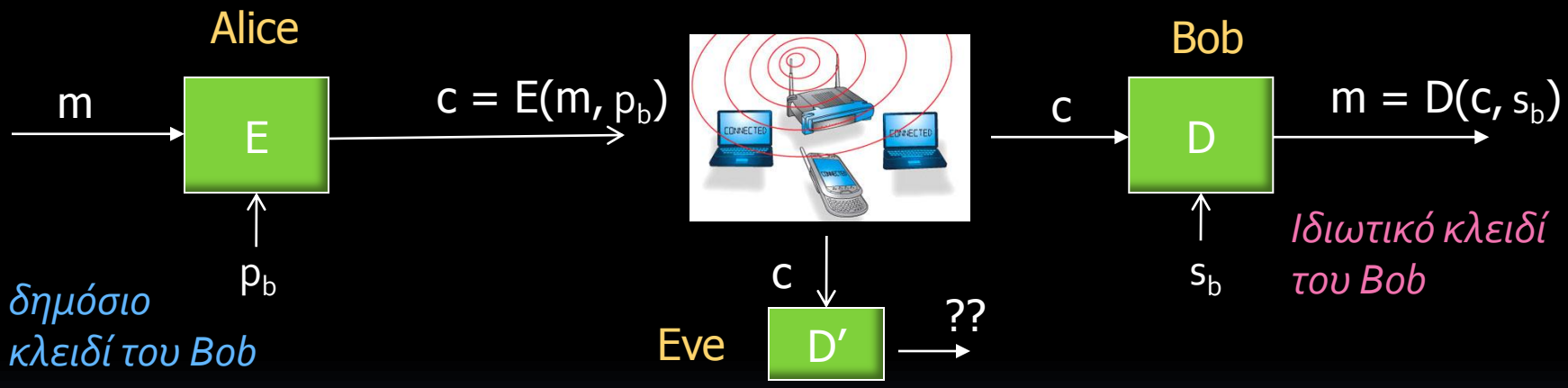
Κρυπτογράφηση Αποκρυπτογράφηση



- … με χρήση *κοινού* ιδιωτικού κλειδιού (συμμετρική κρυπτογραφία)

Μια πρώτη ματιά: ιδιωτικότητα

Κρυπτογράφηση Αποκρυπτογράφηση



- … με χρήση δημοσίου κλειδιού (κρυπτογραφία μονής κατεύθυνσης), μαζί με *απόλυτα* ιδιωτικό, γνωστό στον παραλήπτη μόνο

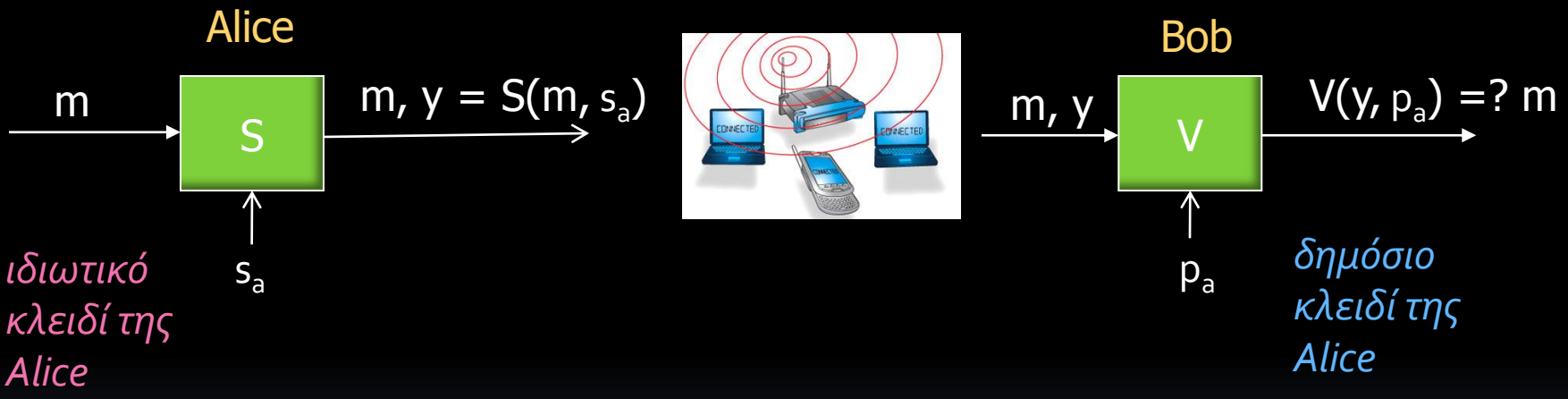
Στην πράξη

- Συνήθης πρακτική
  - Χρήση πρωτοκόλλων ταυτοποίησης για εγκαθίδρυση επικοινωνίας
  - Χρήση κρυπτογραφίας δημοσίου κλειδιού (π.χ. RSA) για ανταλλαγή ιδιωτικού συμμετρικού *κλειδιού συνεδρίας* (session key)
  - Χρήση συμμετρικής κρυπτογραφίας (π.χ. DES, AES) για ανταλλαγή δεδομένων
- Εφαρμογές σε: HTTPS, SSL/TLS, S-MIME, κ.ά.

Μια πρώτη ματιά: υπογραφές

Υπογραφή

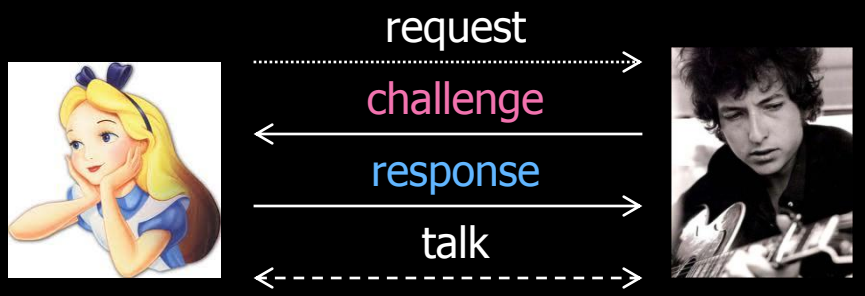
Επαλήθευση



- … με χρήση δημοσίου κλειδιού, μαζί με *απόλυτα* ιδιωτικό, γνωστό στον υπογράφοντα μόνο

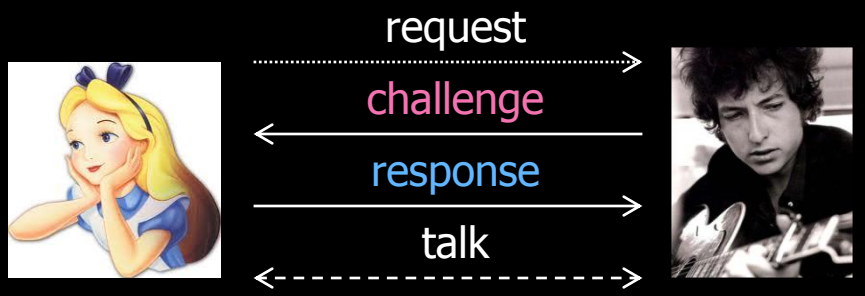
Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση

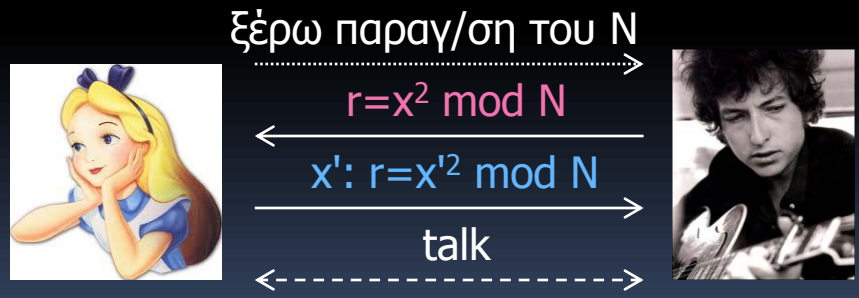


Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση

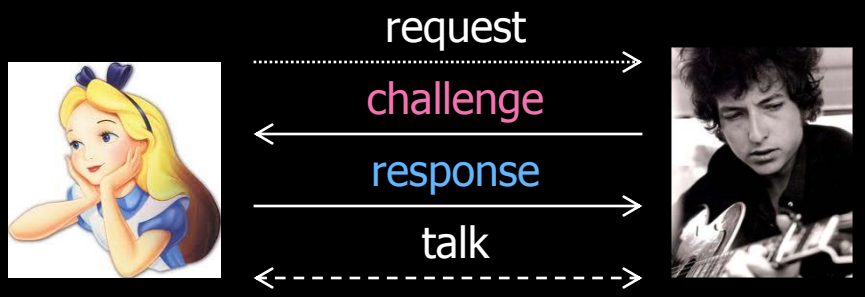


- Αποδείξεις γνώσης

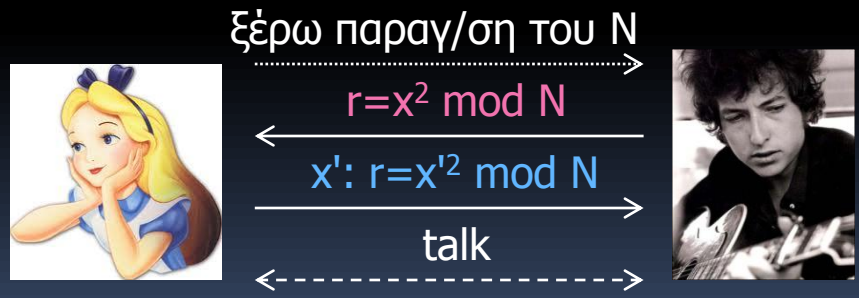


Μια πρώτη ματιά: πρωτόκολλα

- Ταυτοποίηση



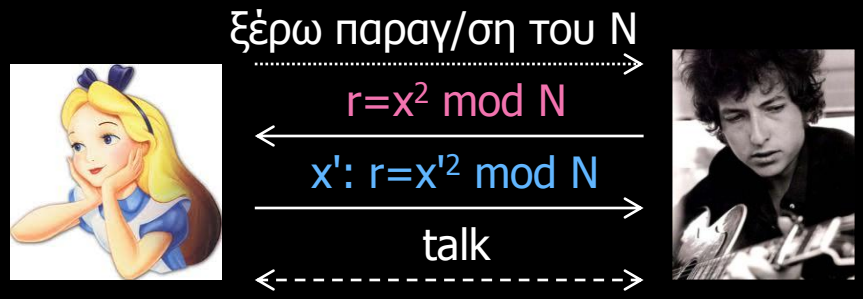
- Αποδείξεις γνώσης



… ακόμη και μηδενικής γνώσης! (πιο περίπλοκο)

Μια πρώτη ματιά: πρωτόκολλα

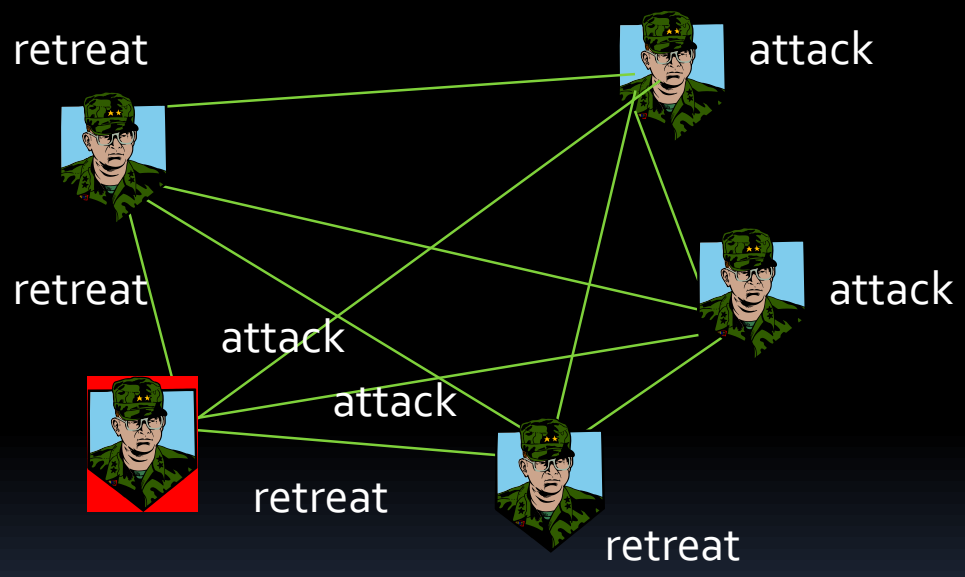
- Μη συνειδητή μεταφορά (oblivious transfer)



- Η Αλίκη δεν ξέρει αν ο Bob έμαθε κάτι ή όχι
- Πολύ σημαντικό πρωτόκολλο

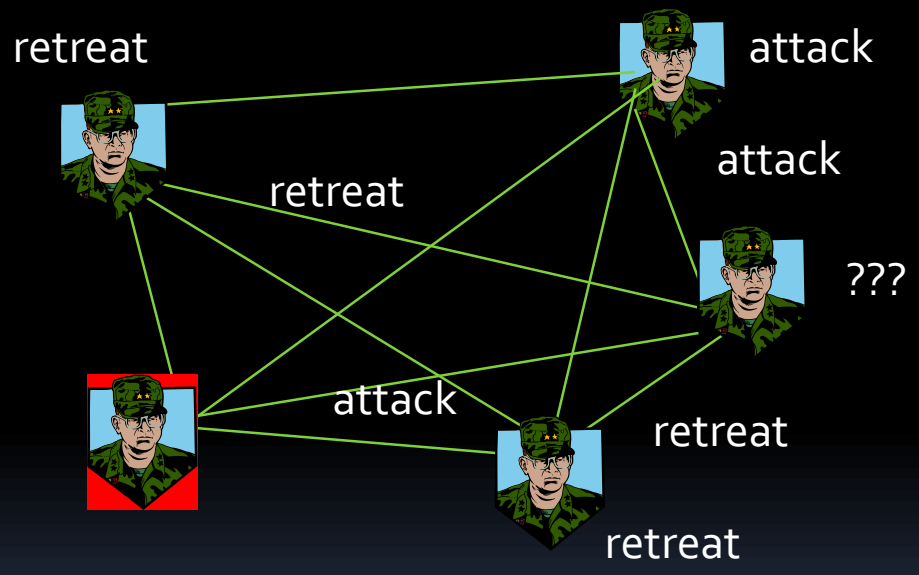
Μια πρώτη ματιά: πρωτόκολλα

- Βυζαντινοί στρατηγοί



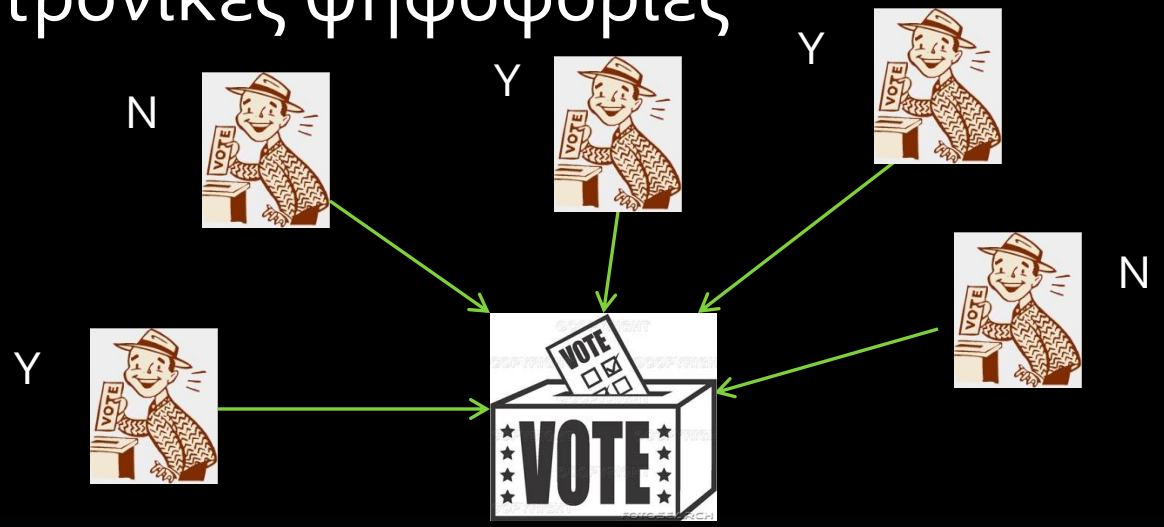
Μια πρώτη ματιά: πρωτόκολλα

- Βυζαντινοί στρατηγοί



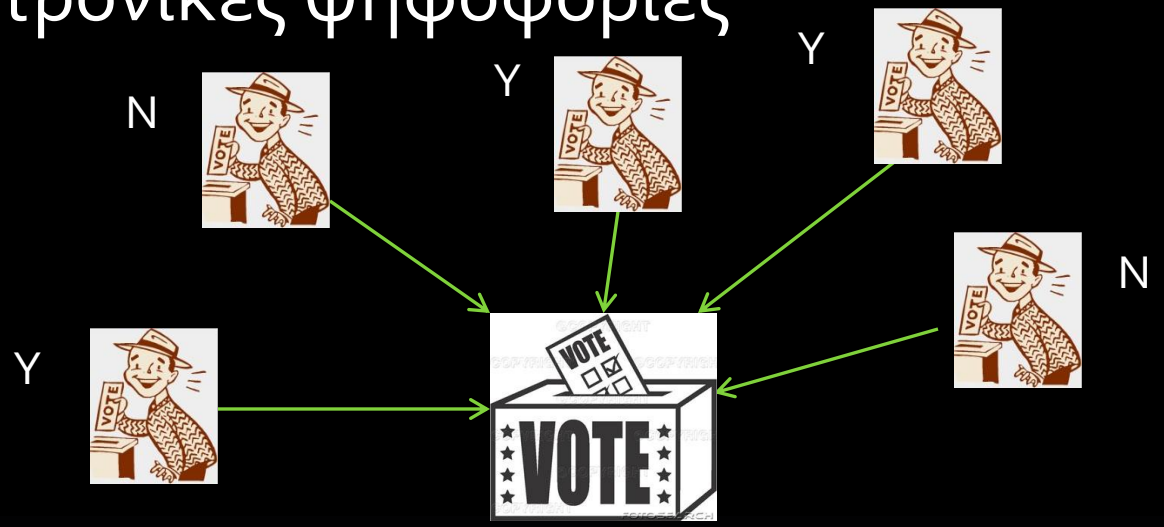
Μια πρώτη ματιά: πρωτόκολλα

- Ηλεκτρονικές ψηφοφορίες



Μια πρώτη ματιά: πρωτόκολλα

- Ηλεκτρονικές ψηφοφορίες



- Secure Multi-Party Computation:
  - *ασφαλής* υπολογισμός $f(x_1, x_2, x_3, x_4, x_5)$

Στόχοι του μαθήματος

- Να εξοικειωθούμε με τις στοιχειώδεις κρυπτογραφικές λειτουργίες και τα πιο σημαντικά κρυπτοσυστήματα
- Να μπορούμε να αναλύσουμε την ασφάλειά τους, σε σχέση και με τις δυνατότητες του αντιπάλου
- Να μπορούμε να επιχειρηματολογήσουμε με αυστηρό τρόπο για τα παραπάνω

Μαθηματικά εργαλεία

- Θεωρία αριθμών
- Άλγεβρα (γραμμική και αφηρημένη)
- Πιθανότητες
- Υπολογιστική πολυπλοκότητα

Πολλά ενδιαφέροντα ανοιχτά προβλήματα!